

DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 18 1994

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

ORIGINAL

In the Matter of
Policies and Rules
concerning Toll Fraud

)
) CC Docket No. 93-292
)

ERRATUM


On January 14, 1994, BellSouth Telecommunications, Inc.
("BellSouth") filed its Comments in the above captioned
rulemaking proceeding. BellSouth inadvertently failed to
attach a copy of Exhibit 1 as referenced in its Comments.

With this filing, BellSouth submits a copy of Exhibit 1
to be incorporated with its Comments.

Respectfully submitted,

BELLSOUTH TELECOMMUNICATIONS, INC.

By:


M. Robert Sutherland
Richard M. Sharatta
Helen A. Shockey

Its Attorneys

4300 Southern Bell Center
675 West Peachtree Street, N.E.
Atlanta, Georgia 30375
(404) 614-4904

Date: January 18, 1994

No. of Copies rec'd
List A B C D E

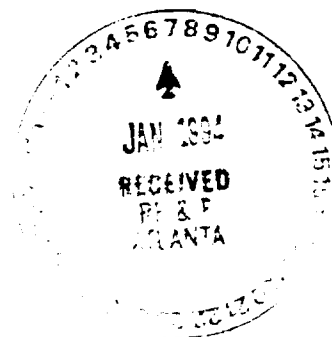
CH9

A Cooperative Solution to the Fraud that Targets Telecom Systems

A Position Paper Developed by the Toll Fraud Prevention Committee of the Network Operations Forum

Sponsored by the Alliance for Telecommunications Industry Solutions

**1200 G Street, NW
Suite 500
Washington, DC 20005
(202) 434-8837**



January 1994

The Toll Fraud Prevention Committee of the Alliance for Telecommunications Industry Solutions (formerly the Exchange Carrier Standards Association) has reviewed the problem of remote access fraud at private branch exchanges (PBXs), voice mail systems, and other customer premise equipment (CPE). Such fraud is a serious liability for business customers (and other customers) of telecommunications services, resulting in hundreds of millions of dollars of losses annually. To date, no one can say with any confidence that a solution has been found, or that the problem is under control.

Remote access fraud involves the penetration of a PBX or other CPE by one or more unauthorized callers, typically for the purpose of gaining access to restricted information or to network facilities where the defrauder cannot be charged for resulting calls. PBX remote access fraud is frequently used for "call sell" operations, where people pay defrauders to place unlimited calls to international destinations. Compromised access codes (800 or local numbers which reach Direct Inward System Access [DISA] ports and maintenance ports in the PBXs) have a commercial value of thousands of dollars in the toll fraud underworld. Criminals have a significant incentive, consequently, to penetrate telecommunications equipment for remote access fraud.

In analyzing this problem the TFPC determined that there are many actual or potential participants involved in providing CPE of every type to telecommunications users. It is reasonable to expect that each party will act responsibly when providing such equipment, to ensure that appropriate security against remote access fraud is included. The TFPC identified the following as industry segments that are involved in this issue:

- the business owner
- the consultant
- sales & installation firms
- original equipment manufacturers
- manufacturers of adjunct equipment
- marketers of secondary/refurbished equipment
- local telephone companies
- long distance carriers
- law enforcement agencies
- legislators
- insurers
- consumer/user groups.

Many of these segments may be involved in an individual CPE configuration. The typical PBX goes through many steps: a needs assessment, equipment evaluation, purchase decision, equipment design, installation and testing, maintenance, ongoing use, and eventual retirement/replacement. Thus, it falls to many parties to evaluate the security of a telecommunications environment at progressive steps in the equipment's life cycle.

With this distribution of responsibility, security is often neglected. This simplifies enormously the task of defrauders, who persistently look for CPE with lax security to use for their illegal purposes. It is necessary to stress that the business owner, the owner or lessee of the CPE, has the primary and paramount care, custody, and control of the CPE.

The owner has the responsibility to protect this asset, the telecommunications system, equally as well as other financial assets of the business. The PBX is vital to the business's health, since virtually every business survives and thrives by communicating with other businesses and customers. Abuse of the PBX by hackers, even to the disruption of its functioning, can carry a significant financial and operational penalty. Consequently, the business owner must assure that the PBX (and the entire telecommunications environment under the owner's control) is secure from penetration and abuse.

It is worth noting that this form of telecommunications fraud is a crime. Businesses, whether small firms or large corporations, are persons before the law. They also enjoy the same protections as other citizens, including protection from unlawful disruption of their operations and from theft. Therefore, defrauders of these corporate citizens should be prosecuted to the full extent of the law.

It is essential, therefore, that every industry segment support the integration of security into PBXs, voice mail systems, and other CPE. Some segments have a direct role, as is the case for the equipment manufacturer and the installation firm. Others, such as legislators and regulators, have a less direct, but still important role in the control of toll fraud in general, and remote access fraud in particular. The attachment to this position paper outlines the recommendations of the TFPC for each segment of the industry. For each there is a minimal requirement for preventive action, supported by additional steps that each party should take. These recommendations are not exhaustive of all preventive steps, nor will those that are adopted end remote access fraud. However, they will reduce the risks that industry currently faces.

In the judgment of the TFPC, coordination and cooperation are essential to achieving greater success in this area. Consequently, the TFPC urges each industry segment to deliver the maximum protection that it can identify, in supporting customers of telecommunications services.

ATTACHMENT: SUGGESTED ANTI-FRAUD EFFORTS BY INDUSTRY SEGMENT

RESPONSIBILITIES OF THE BUSINESS OWNER:

The basic responsibility of the business owner is to devote adequate resources (time, talent, capital, etc.) to the selection of CPE and to its management, including fraud prevention, detection, and deterrence. It is an essential part of managing the business. The owner must demand that internal staff and supporting external professionals, such as consultants, include security concerns in the evaluation, design and operation of the telecommunication environment for his/her business.

Other efforts are highly recommended to assure that security matches the importance placed on efficiency, economy, accountability, etc., as considerations in PBX and CPE design.

- Enlist knowledgeable professional support (consultants, security experts) as needed.
- Include security as a prime consideration in the definition of system and user needs.
- Require suppliers to provide only the capabilities required/requested. Other features should be made known, with controls, restrictions, vulnerabilities clearly noted.
- Include security support in maintenance agreements. Identify emergency telephone numbers to be used on discovery or suspicion of fraudulent abuse.
- Define and implement an anti-fraud plan. Enlist employees in the plan; provide a feedback system for emergency alerts. Monitor and refine the plan.
- Manage the telecommunications system when installed: monitor usage continually; assign and encrypt passwords; restrict access in, out, and between interconnected nodes of the system; assure the compatibility and security of interconnected CPE.
- Enlist law enforcement agencies when victimized; preserve evidence for prosecution.
- Secure relevant documentation, to avoid compromise and piracy of data, passwords, etc.
- Secure access to the physical facilities, cabling, access ports, administrative terminals, etc.

RESPONSIBILITIES OF THE CONSULTANT:

The consultant supports the business owner in deciding what type of equipment to buy, what type of services to install, and how to configure both equipment and services for

the desired operational environment. It is the consultant's responsibility frequently to act in place of the owner. Consequently, the consultant has the same tasks as the owner. Trusted for special expertise, the consultant must place high among his/her priorities the establishment of a secure telecommunications environment. This requires that the consultant be very aware of any fraud implications regarding the system being recommended, and ensure that others involved (vendors, installation technicians, etc.) meet or exceed the levels of security needed. The consultant should take steps to ensure that security is cared at the time of installation and into the future.

Additional support efforts are appropriate:

- Understand all current fraud exposures with CPE, and know how to minimize, if not prevent, exposure in the current telecommunications environment.
- Consider security features when making a recommendation on equipment, and detail in writing to the owner the fraud exposure of the final configuration.
- Understand how features in the local and long distance carriers' services can be used to enhance the security of the equipment.
- Be knowledgeable of and make the owner aware of adjunct equipment that can help prevent and identify abuse.

RESPONSIBILITIES OF THE SALES AND INSTALLATION FIRMS:

The sales and installation firms, which will frequently provide ongoing service and maintenance of the CPE, should assist in educating the business owner about the risks and vulnerabilities of the equipment. While stressing the value of the system's features, the sales agents should make known the dangers of toll fraud.

Additional support efforts are appropriate:

- Be completely familiar with the system's features, including those subject to compromise and abuse, such as DISA, maintenance ports, least cost routing features, etc.
- Identify and change any default codes that control access to features and facilities that are subject to compromise and abuse. Secure such replacement codes with responsible management personnel.
- Deactivate features that are not needed, with the full knowledge of the customer.
- Establish time of day restrictions, such as no access to international calling at night and on weekends.
- Restrict access to facilities (WATS, public network "dial 9") and establish calling privileges/limits (internal, local, domestic, international) as appropriate.

RESPONSIBILITIES OF THE MANUFACTURERS OF ORIGINAL AND ADJUNCT EQUIPMENT AND THE MARKETERS OF SECONDARY/REFURBISHED EQUIPMENT:

These industry segments play a special role in protecting the industry from toll fraud. These manufacturers must develop and deploy flexible and effective security protections to complement the advanced telecommunications features required by businesses. In many cases customers are not aware of the need for such protections and do not request them. They are often unaware of the vulnerabilities of an unprotected system and of the dogged drive of the hacker to find new PBXs to abuse.

Additional support efforts are appropriate:

- List in writing for the customer the features and treatments that are necessary to protect against PBX compromise and abuse.
- Ship only those features that the customer requests; remove default passwords from features such as DISA, so that hackers cannot easily access them.
- Secure in writing that the customer is aware of the system's capabilities and protections.
- Provide emergency contact numbers for customers to use in cases of compromise and abuse.
- Make upgrades to the CPE's controlling software by methods more secure than a dial-up modem with default passwords. For example, update the customer's CPE through call back modems or secure token access devices.
- Care for the security and compatibility of adjunct and refurbished equipment with other interconnected segments of the customer's network.
- Educate the customer thoroughly, including support for user groups, etc.

RESPONSIBILITIES OF THE LOCAL TELEPHONE COMPANIES:

The local telephone companies (LECs) have a supporting role for customers who choose their own PBX and CPE. The LECs may frequently not know what a customer is planning. Nor are the LECs familiar with the wide variety of terminal equipment that is available to business owners. However, they can help to combat fraud by promoting an heightened security concern among all their customers.

Other suggested efforts include:

- Conduct wide customer education through bill inserts, addressing end user groups, holding training seminars, etc.
- Evaluate permitted teaming efforts with long distance companies, equipment manufacturers, etc. to educate customers.
- Evaluate all LEC products and services for security concerns before deployment.

- Where tariffed telecommunications systems are offered, fulfill the above suggested security functions of manufacturer and consultant, as appropriate.
- Alert their customer contact personnel (business office, repair, sales/service) to the signs of toll fraud, so that these staffs can better support business owners who are victimized.
- Deploy network blocking services (such as International Direct Dial Blocking) and call screening information digits to complement customer equipment restriction strategies and long distance company network monitoring.
- Develop network monitoring capabilities to highlight potential fraud patterns (local hacking, 800, international, etc.) as early as possible.
- Expand centralized fraud bureau support to a seven day/24 hour basis.
- Continue the use of security staffs to support long distance company investigations and customer inquiries.
- Cooperate with law enforcement agencies in education, investigation, and prosecution efforts.
- Develop case documentation for federal and local regulators, in support of guidelines allowing timely and responsive security efforts in cases of toll fraud.

RESPONSIBILITIES OF THE LONG DISTANCE COMPANIES:

The long distance companies (IXCs) are frequently the networks that bear the brunt of toll fraud, because fraudulent calls are often directed to international destinations. IXCs assist in protecting their customers with a variety of monitoring capabilities and protection (indemnity) plans. IXCs also can combat fraud by continuing the extensive educational campaigns to all customers.

Other suggested efforts include:

- Perform network monitoring of 800 calling and calls directed to international destinations, to identify suspected fraud patterns.
- Alert their customer contact personnel (business office, operator services, repair, sales/service) to the signs of toll fraud, so that these staffs can better support business owners who are victimized.
- Include in their network sales efforts educational security information that will alert customers to network vulnerabilities and suggest effective protections.
- Continue the use of security staffs to support customer inquiries.
- Cooperate with law enforcement agencies in education, investigation, and prosecution efforts.
- Develop case documentation for federal and local regulators, in support of guidelines allowing timely and responsive security efforts in cases of toll fraud.

RESPONSIBILITIES OF REGULATORS:

Regulators perform a critical task in defining how the market acts and reacts. In the case of toll fraud, regulators should recognize that it costs the telecommunications industry (and ultimately consumers and shareholders) billions of dollars annually. Those best able to combat fraud should be empowered to take timely and effective steps to minimize its incidence and severity. In some cases regulatory guidelines might appear to prevent LECs and/or DXCs from disconnecting defrauders in a timely manner. Companies that operate across many states are frequently subject to conflicting rules that do not reflect the realities of systematic, professional toll fraud. Confusion over rules covering collection and security activities allows defrauders to stay on the network. Regulators should act to clarify such areas.

Additional suggestions are:

- Cooperate across jurisdictions (e.g., through NARUC, the FCC) to standardize regulations that allow timely and effective responses against toll fraud.
- Alert customers through periodic press releases about the vulnerabilities of toll fraud and their responsibilities to take effective precautions.
- Stimulate effective legislation punishing toll fraud, and promote its enforcement.
- Allow LECs to deny service, both before it is established and after installation takes place, when warranted by suspected fraud.
- Allow telecommunications service providers to cooperate in combating toll fraud through the exchange of customer information.

RESPONSIBILITIES OF LEGISLATORS:

Legislators help create the telecommunications environment in response to the drive of technology and market forces. It is essential that they foster a legislative environment in which telecommunications service providers can bring their full skills to the prevention, detection, and deterrence of toll fraud, recognizing that toll fraud is a professional endeavor that continually adapts.

Other steps are:

- Create no anti-fraud mandates that pit segments of the industry against each other, or that allow one segment to avoid responsibility for contributing to the solution.
- Create incentives for the industry to work cooperatively against the problem.
- Support and finance the efforts of law enforcement organizations, so that they are empowered to pursue and prosecute perpetrators of toll fraud.
- Amend the penal codes to remove the relative impunity enjoyed by those who engage in toll fraud as a profession.

RESPONSIBILITIES OF INSURERS:

Insurers can expand the attention that toll fraud receives by including coverage for toll fraud liability in their product portfolios. Insurers can contribute greatly to the education of business customers by discussing risks and protections related to toll fraud, together or separately with other risk coverage that virtually all businesses consider. Packaging and pricing toll fraud liability coverage affordably (yet profitably) will prompt businesses to take effective precautions. This, in turn, will reduce the incidence of remote access fraud.

RESPONSIBILITIES OF END USER GROUPS:

Trade associations and telecommunications end user groups can also broadcast that toll fraud is a significant risk for businesses. Education from many sides will reinforce the necessity for protective action. User groups are particularly valuable in this mode. Frequently, they are aligned by their use of a single technology or a single vendor. Consequently, they can readily share both negative experiences and effective remedies. These groups can also provide the "critical mass" needed to stimulate development of new technology.

RESPONSIBILITIES OF LAW ENFORCEMENT AGENCIES:

While toll fraud might appear as a victimless crime, or one of less pressing priority for prosecution, nevertheless, the operational and financial harm done to businesses by telecommunications defrauders is substantial. Federal and state laws variously define telecommunications fraud and place enforcement responsibilities in many organizations. It is important that this distribution not hinder timely investigations and effective enforcement. Police officers should cooperate across jurisdictions to investigate suspected cases, and district attorneys should prosecute cases to deter future toll fraud and gain restitution for victimized businesses. The enforcement community can also aid the essential educational effort through its own support of end user groups, business councils, etc.